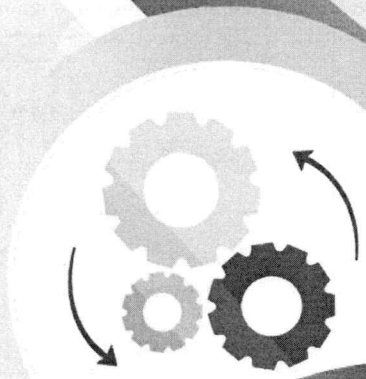
HOSPITAL DEL SARARE
Empresa Social del Estado

INFORME SEGUIMIENTO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (SIS-01-R03) Y PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACIÓN (SIS-01-R04) I CUATRIMESTRE 2026

SEGUIMIENTO INSTITUCIONAL
CONTROL INTERNO



Sistema Integrado de Gestión

1. Tabla de Contenido

Tabla de contenido

2. Introducción

Atendiendo uno de los propósitos del sistema de Control Interno, el cual está orientado a lograr la eficiencia, eficacia y transparencia en el ejercicio de las funciones de la entidad, la Oficina de Control Interno dando cumplimiento a la Ley 87 de 1993, Decreto 1068 de 26 de mayo de 2015, Decreto 371 de 2021 del 08 de abril del 2021 y Decreto 3036 de 2016 Art 16; presenta Informe de seguimiento al Plan de Seguridad y privacidad de la información y al plan de tratamiento de riesgos primer cuatrimestre de la vigencia 2026 en lo relacionado a la Política de Seguridad Digital del MIPG.

3. Objetivo del Informe

Verificar la implementación del Plan de seguridad y privacidad de la información, así como el avance del seguimiento a los tratamientos de riesgos de seguridad de la información para la vigencia en el marco de los lineamientos de la política MIPG Seguridad digital con alcance al primer cuatrimestre de la vigencia 2026

4. Línea estratégica y normativa

- Estrategia nacional de Seguridad digital de Colombia 2025-2027
- Resolución No 02277 del 03/06/2025 de Mintic por el cual se Actualiza el anexo 1 de la Resolución 500 del 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de las políticas de Gobierno digital.
- Decreto 767 de 2022 Por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 338 de 2022 Fortalece la gobernanza de la seguridad digital en Colombia.
- Decreto 620 de 2020 reglamenta parcialmente la Ley 1437 de 2011 y establece lineamientos para el uso y operación de los servicios ciudadanos digitales en Colombia.
- Resolución 500 del 2021 establece lineamientos y estándares para la estrategia de seguridad digital y adopta un modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital en Colombia.
- Documentos CONPES 3701 de 2011, 3854 de 2016 y 3995 de 2020, los cuales han guiado la política de seguridad digital del país en la última década.
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Ley Estatutaria 1712 de 2014 por medio del cual se crea la Ley de Transparencia y del derecho de acceso a la información pública Nacional y se dictan otras disposiciones.
- Modelo Integrado de Planeación y Gestión (MIPG)

5. Metodología

El seguimiento se realiza a través de las siguientes actividades:

- Verificación de la información documentada.
- Solicitud de información al subproceso de Gestión de las tecnologías y sistemas de información
- Revisión de los resultados de la ESE Hospital del Sarare en el FURAG vigencia anterior.
- Registros de información al subproceso de Gestión de las tecnologías y sistemas de información.
- Información publicada en la página web institucional
- Verificación de la metodología gestión por procesos

6. Resultados del seguimiento

6.1 Política Nacional Gobierno Digital

Revisión marco normativo según Decreto 0767 del 2022:

Artículo 2.2.9.1.1.2. Ámbito de aplicación. Los sujetos obligados a las disposiciones contenidas en el presente Capítulo serán las entidades que conforman la administración pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas.

PARÁGRAFO. La implementación de la Política de Gobierno Digital en las ramas legislativa y judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política.

Artículo 2.2.9.1.3.2. Responsable Institucional de la Política de Gobierno Digital. El representante legal de cada sujeto obligado, o quien haga sus veces, será el responsable de coordinar, adoptar, implementar y hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital en su respectiva entidad.

Artículo 2.2.9.1.3.3. Responsable de orientar la implementación de la Política de Gobierno Digital. Los Comités Institucionales de Gestión y Desempeño de que trata el artículo 2.2.22.3.8 del Decreto 1083 de 2015, serán los responsables de orientar la implementación de la Política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Artículo 2.2.9.1.3.4. Responsable de liderar la implementación de la Política de Gobierno Digital. El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, del respectivo sujeto obligado, tendrá la responsabilidad de liderar la implementación y la mejora continua de la Política de Gobierno Digital. Las demás áreas de la entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

De acuerdo a lo anterior se verificó y la ESE cuenta con:

- Se realizó verificación en la página web institucional y no se identificó documentó relacionado con la adopción de la política gobierno digital.

https://hospitaldelsarare.gov.co/publicaciones/normas,-procedimientos-y-lineamientos/politicas.html

- Se realizó verificación en la página web institucional y se identificó documento Plan Estratégico de las tecnologías de la información PETI el cual en el alcance incluye... *aplica para todos los procesos que contribuyen al desarrollo de los recursos de tecnologías de información y dando cumplimiento con los lineamientos que establece la política de Gobierno Digital, siendo susceptible de ajustes a corto y mediano plazo para implementar en la Entidad.*

https://hospitaldelsarare.gov.co/images/publicaciones/Planeacion/TICS/PETI/PETI-ESE-HOSPITAL-DEL-SARARE-2024.pdf

Dicho documentó requiere actualización ya que está basado en el Decreto Nacional 2573 de 2014 el cual fue derogado por el Decreto 0767 del 2022.

- PETI incluye proyectos a desarrollar en el Cuatrenio que define el PETI 2024-2027:

BENEFICIOS ESPERADOS	VERIFICACIÓN
Contar con una ruta guía para el logro de la optimización de los procesos, basados en directrices del Gobierno Digital, con el fin de brindar mejoras en los servicios de tecnología de la información enfocada en los usuarios.	No se identificó
Cumplimiento de los lineamientos de Gobierno en Digital. Actualización de la plataforma de red. Mejoramiento de la seguridad de red. (Indicador Números de servidores y Pc con soporte a red IPv6 / Número Total de Servidores + PC)	En el plan de acción 2026 se identifica la actividad de Plan de diagnóstico para la transición de IPv4 a IPv6.
Separar el Gobierno de la Gestión de TIC con el proceso de seguridad de la información, dando cumplimiento de la norma. Plan de acción.	Plan de acción no incluye actividades para la política gobierno digital.

CONCLUSIÓN:

Se evidencia necesidad de actualización documental teniendo en cuenta el Decreto 0767 del 2022 y la Resolución No 02277 del 03/06/2025 de Mintic por el cual se Actualiza el anexo 1 de la Resolución 500 del 2021 estableció actualizaciones en los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de las políticas de Gobierno digital.

Basado en el Plan de diagnóstico para la transición de IPv4 a IPv6 encontrándose la entidad debe generar las acciones de mejora siendo fundamental el seguimiento a estas a través del comité de gestión y desempeño, así como a la gerencia de la entidad.

6.2 Políticas institucionales

6.2.1 Política de seguridad de la información

Se realizó verificación en la página web institucional y se identifica acto administrativo No 065 del 15/03/2021.

HOSPITAL DEL SARARE
Empresa Social del Estado
NIT. 800231215-1
Evolucionamos pensando en usted

Vigilado Supersalud

Ministerio de la Protección Social
Departamento de Arauca

Resolución No 065 de 15 de Marzo de 2021.

"Por la cual se adopta la Política de Seguridad Digital"

EL GERENTE DE LA E.S.E HOSPITAL DEL SARARE en uso de sus facultades y

CONSIDERANDO:

Que el Hospital del Sarare Empresa Social del Estado, es una entidad púbica descentralizada del Orden Departamental, de conformidad con lo propuesto en el artículo 194 de la Ley 100 de 1993 y de la ordenanza Nro. 07E de 2008, que modifica los artículos 2 y 4 y el parágrafo 2 de la ordenanza

https://hospitaldelsarare.gov.co/images/publicaciones/politicas/RESOLUCION-N-065-POLITICA-SEGURIDAD-DIGITAL.pdf

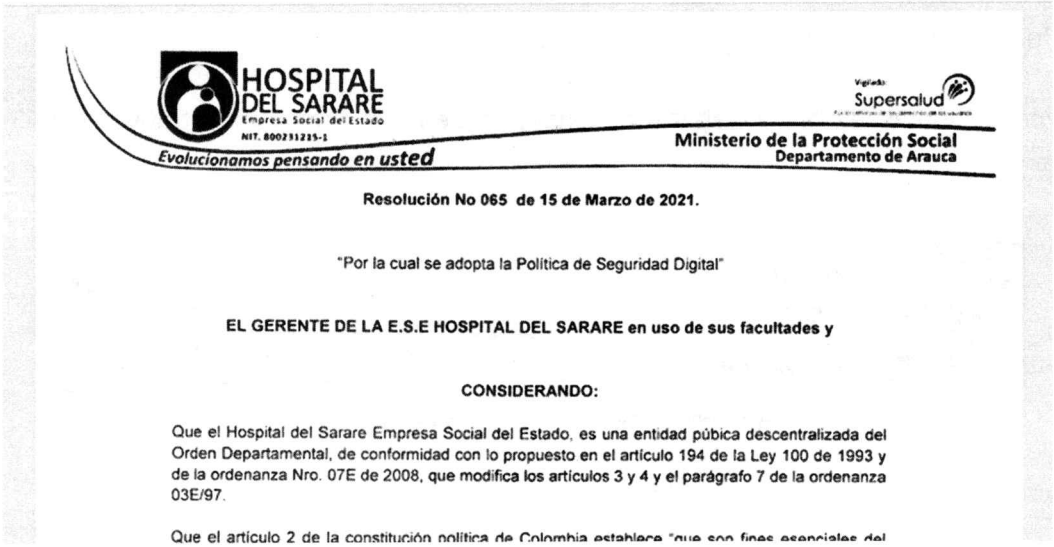
CONCLUSIÓN:

Se evidencia necesidad de actualización debido a la expedición por Mintic de la RESOLUCIÓN 02277 DE 2025 Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

En plan de acción 2025 se evidenció planeación de la actividad Plan de diagnóstico para la transición de IPv4 a IPv6, no se evidenciaron actividades planeadas o ejecutadas de la política de seguridad de la información como capacitaciones socializaciones.

6.2.2 Política de seguridad digital

https://hospitaldelsarare.gov.co/images/publicaciones/politicas/RESOLUCION-N-065-POLITICA-SEGURIDAD-DIGITAL.pdf



HOSPITAL DEL SARARE
Empresa Social del Estado
NIT. 800231215-1
Evolucionamos pensando en usted

Vigilado Supersalud

Ministerio de la Protección Social
Departamento de Arauca

Resolución No 065 de 15 de Marzo de 2021.

"Por la cual se adopta la Política de Seguridad Digital"

EL GERENTE DE LA E.S.E HOSPITAL DEL SARARE en uso de sus facultades y

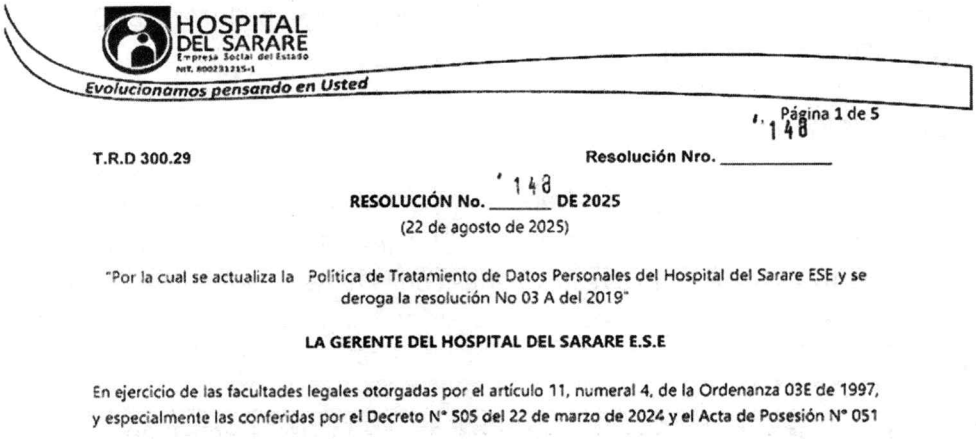
CONSIDERANDO:

Que el Hospital del Sarare Empresa Social del Estado, es una entidad púbica descentralizada del Orden Departamental, de conformidad con lo propuesto en el artículo 194 de la Ley 100 de 1993 y de la ordenanza Nro. 07E de 2008, que modifica los artículos 3 y 4 y el parágrafo 7 de la ordenanza 03E/97.

Que el artículo 2 de la constitución política de Colombia establece "que son fines esenciales del

6.2.3 Política de protección de datos personales

Se realizó verificación en la página web institucional y se identifica acto administrativo No 148 del 2025.



HOSPITAL DEL SARARE
Empresa Social del Estado
NIT. 800231215-1
Evolucionamos pensando en Usted

Página 1 de 5

T.R.D 300.29 **Resolución Nro. 148**

RESOLUCIÓN No. 148 DE 2025
(22 de agosto de 2025)

"Por la cual se actualiza la Política de Tratamiento de Datos Personales del Hospital del Sarare ESE y se deroga la resolución No 03 A del 2019"

LA GERENTE DEL HOSPITAL DEL SARARE E.S.E

En ejercicio de las facultades legales otorgadas por el artículo 11, numeral 4, de la Ordenanza 03E de 1997, y especialmente las conferidas por el Decreto N° 505 del 22 de marzo de 2024 y el Acta de Posesión N° 051

https://hospitaldelsarare.gov.co/images/publicaciones/politicas/2025/politicadettodedatos/Actualizacion-Politica-Tratamiento-de-Datos.PDF

Vigilado Supersalud

CONCLUSIÓN:

Se evidencia correcto estado de actualización marco normativo Decreto 255 del 2022.

La ESE documentó en la vigencia 2025 el Manual de políticas y procedimientos Habeas data SIS-01-M02 el cual fue aprobado mediante el comité de Gestión y desempeño el 28 de mayo del 2025.

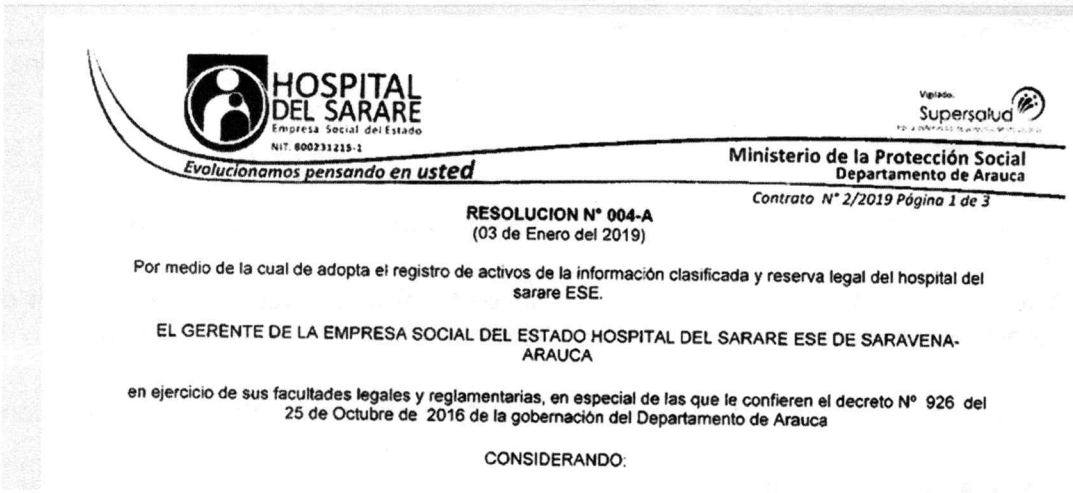
Se evidencia plan de mejoramiento en el marco de Auditoría interna de Riesgos y del consultor.

7. Planes institucionales

Se evidencia SIS-01-R03 Plan de seguridad y privacidad de la información aprobado el 30-11-2021 mediante el comité de Gestión y desempeño, el plan tiene como objetivo definir las actividades para la implementación del Modelo de Seguridad y Privacidad de la Información MSPI del Hospital del Sarare.

CONCLUSIÓN:

- El documento se relaciona con la política de seguridad y privacidad de la información acto administrativo No 065 del 15/03/2021 el cual requiere actualización.
- Rol y responsabilidades del MSPI: es necesario fortalecer el seguimiento a través del comité de Gestión y seguimiento.
- Identificación de activos de información: cuenta con inventario el cual es reportado en los diferentes informes normativos y en el modulo de inventarios del software de dinámica gerencial.
- Clasificación de los activos de información: se evidencia acto administrativo de registro de activos de información clasificada y de reserva legal. RESOLUCION--N-004-A-RESERVA-LEGAL-20190830 17574750 .pdf El cual amerita su revisión y verificación de estado de actualización.



HOSPITAL DEL SARARE
Empresa Social del Estado
NIT. 800231215-1
Evolucionamos pensando en usted

Vigilado Supersalud

Ministerio de la Protección Social
Departamento de Arauca

Contrato N° 2/2019 Página 1 de 3

RESOLUCION N° 004-A
(03 de Enero del 2019)

Por medio de la cual de adopta el registro de activos de la información clasificada y reserva legal del hospital del sarare ESE.

EL GERENTE DE LA EMPRESA SOCIAL DEL ESTADO HOSPITAL DEL SARARE ESE DE SARAVENA-ARAUCA

en ejercicio de sus facultades legales y reglamentarias, en especial de las que le confieren el decreto N° 926 del 25 de Octubre de 2016 de la gobernación del Departamento de Arauca

CONSIDERANDO:

- Plan de tratamiento de riesgos de seguridad y privacidad de la información: la ESE ha creado el subproceso de Gestión y administración del riesgo por lo cual es fundamental la articulación ya que se están dando actualizaciones del manual institucional de administración de riesgos.
- Documentación del MSPI
  El Plan incluye documentar lo siguiente:
  - Procedimiento y/o guía de identificación y clasificación de activos de información.
  - Procedimiento Continuidad del Negocio.
  - Procedimientos operativos para gestión de TI
  - Procedimiento para la gestión de eventos e incidentes de seguridad de la información
  - Procedimiento para la gestión de vulnerabilidades de seguridad de la información.

- Competencia toma de conciencia y comunicación: se requiere la articulación con Comunicación e imagen corporativa para las acciones de sensibilización, educación a funcionarios de la entidad para dar a conocer su rol, responsabilidad, consecuencias de incumplimiento de políticas y lineamientos en lo relacionado a la seguridad y privacidad de la información.

Se evidencia SIS-01-R04 Plan de Tratamiento de Riesgos y seguridad y privacidad de la información aprobada el 30-11-2024 mediante el comité de Gestión y desempeño.

CONCLUSIÓN:

- Se relaciona con la política de gestión y control de riesgos Resolución 259 del 23/11/2017 la cual la entidad actualizó mediante la Resolución No 205 del 2024 publicada en https://hospitaldelsarare.gov.co/images/publicaciones/politicas/RESOLUCIN-205---

RIEGOS.pdf generando la necesidad de actualización del Plan. En dicha actualización se recomienda tener en cuenta la Guia de administración de riesgo V7 de Función pública.

- Implementación: el plan menciona su ejecución y seguimiento a través del comité de gestión y desempeño, pero al realizar verificación de las actas suscritas por el comité en el 2025 no se evidenció seguimiento a dicho plan. Sin embargo, se evidenciaron revisión resultados de la política FURAG y mejoras identificadas.

8. Resultados FURAG 2025

Aun no han salido los resultados de la Evaluación de Desempeño Institucional de la vigencia 2025, se espera que para el II cuatrimestres se tengan los resultados con sus recomendaciones.

9. MATRIZ DE RIEGOS

Nº DE RIESGO	TIPO DE RIESGO	SISTEMA	PROCESO	SUBPROCESO	DESCRIPCIÓN DEL RIESGO	FRECUENCIA CON LA CUAL SE REALIZA LA ACTIVIDAD	PROBABILIDAD INHERENTE
48	Riesgos de Seguridad de la Información	Subsistema de administración del riesgo operativo	gestión_INTEGRAL_DE_LA_información	Gestión de las Tecnologías y Sistemas de Información	Posibilidad de perdida de confidencialidad, integridad y/o disponibilidad de la información por acceso no autorizado a la información de pacientes, empleados contratistas, proveedores, donantes de sangre a causa de Obsolescencia y brechas de seguridad por uso de versionamiento desactualizado del entorno de los diferentes sistemas de información. (gestión tecnologías e información) (Seguridad de la información)	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	Muy Baja
49	Riesgos de Seguridad Digital	Sistemas Integrados de Gestión	gestión_INTEGRAL_DE_LA_información	Gestión de las Tecnologías y Sistemas de Información	Posibilidad de perdida de disponibilidad por fallas en la conectividad a causa de Falta de reingeniera de la Red de Datos y migración a IPV6 (gestión tecnologías e información) (Seguridad de la información)	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	Media
50	Riesgos de Seguridad de la Información	Subsistema de administración del riesgo operativo	GESTION_INTEGRAL_DE_LA_INFORMACION	Gestión de las Tecnologías y Sistemas de Información	Posibilidad de perdida de disponibilidad de información a causa de no contar con servidores espejo o copias de seguridad sin condiciónes adecuadas de preservación (gestión tecnologías e información) (Seguridad de la información)	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	Alta

Ilustración 1 Matriz de Riesgos Institucional 2026

Para el Primer Cuatrimestre del año 2026, se gestionaron los riesgos establecidos en la Matriz de Riesgos de seguridad de la información, la cual hace parte del Mapa de Riesgos Institucional Versión 2, lo cual esta disponible para la consulta en la IP4 \\192.168.1.4\lideres-sig\11. GESTION DE RIESGO\2026\MAPA DE RIESGOS INTEGRAL.

Se relacionan los riesgos y sus controles:

Riesgo 1:
Posibilidad de pérdida de confidencialidad, integridad y/o disponibilidad de la información por acceso no autorizado a la información de pacientes, empleados contratistas, proveedores, donantes de sangre a causa de Obsolescencia y brechas de seguridad por uso de versionamiento desactualizado del entorno de los diferentes sistemas de información. (gestión tecnologías e información) (Seguridad de la información).

Control: Es responsable de que existan copias de seguridad de la intranet y la información cargada del usuario en el software de dinámica

Riego 2:
Posibilidad de pérdida de disponibilidad por fallas en la conectividad a causa de Falta de reingeniería de la Red de Datos y migración a IPV6 (gestión tecnologías e información) (Seguridad de la información)

Control: Realizar trabajo de migración de IPV4 a IPV6

Riesgo 3:
Posibilidad de pérdida de disponibilidad de información a causa de no contar con servidores espejo o copias de seguridad sin condiciones adecuadas de preservación (gestión tecnologías e información) (Seguridad de la información)

Control: Se realizan backup cada 12hrs

Masterización de Riesgos:
Durante el Primer Cuatrimestre de 2026 la Oficina de Tecnologías de la información y las comunicaciones NO recibió alertas correspondientes a la posible materialización de riesgos de Seguridad de la información.

10. AUDITORIA INTERNA

Para el mes de abril de la vigencia 2026 se realiza Auditoria Interna la cual tiene un porcentaje del 60% de cumplimiento, se efectúa el levantamiento del plan de mejora y se suscriba e implementen las acciones que conllevan a contrarrestar los hallazgos y/o observaciones presentadas mediante la Auditoria.

11. Recomendaciones

✓ Realizar revisión del marco normativo vigente y aplicable a la entidad y basado en este realizar la actualización documental.
✓ Articular los planes con el Subproceso de Gestión y administración de riesgos para promover la integralidad de la información en la entidad.
✓ Realizar depuración actualización de la información publicada en la página web institucional relacionada con la seguridad y privacidad de la información y riesgos en el ciclo PHVA.
✓ En el marco del comité de Gestión y desempeño realizar seguimiento a la política de gobierno digital y seguridad de la información.
✓ Realizar seguimiento trimestral en la matriz de riesgos.

12. Glosario de Términos

Se remite a los Términos y definiciones de seguridad de la información y seguridad digital de la Contaduría General de la Nación VS 15/11/2024.
https://www.contaduria.gov.co/documents/d/guest/40-terminos-y-definiciones-de-seguridad-de-la-informacion

12. Control de Elaboración

Revisó	Yenny Carolina Suarez Asesor Control Interno	
Realizó	Geraldine Real Lozano Profesional Univ. Apoyo Control Interno	